資料５

意見書

2023 年 7 月 4 日
日本電気株式会社
特別顧問
遠藤　信博

DX の進展、さらには国際情勢の急激な悪化といった状況により、サイバー犯罪・サイバー攻撃は増加傾向が続いています。このような情勢の中、サイバーセキュリティ 2023(案)を取りまとめて頂き感謝いたします。我々が遭遇している多種多様なリスクにしっかり対応したセキュリティ計画だと思います。また、政府機関等のサイバーセキュリティ対策のための統一基準群(案)、重要インフラのサイバーセキュリティに係る安全基準等策定指針(案)の内容に関しても、特に異論はありません。

1. サイバーセキュリティ 2023

サイバー攻撃に対する防御という言葉からは、高度なテクニックを駆使した防御が連想されますが、実際のサイバー攻撃防御の要諦は「基本的な対策」を繰り返し実行する極めて地味な活動にあると思います。サイバーセキュリティ 2023 においても、セキュリティの基本をおろそかにしない姿勢が高く評価できると思います。セキュリティの基本の中で特に重要なのは「最も弱いところを強化する」ということで、これは「攻撃者視点」で対策を考えることにもつながっています。

今までのサイバーセキュリティ対策は、平時におけるサイバー攻撃を想定し、その防御方法を練ったものでした。しかし、世界の現状は、ウクライナが軍事侵攻を受け、アジアでも緊張感が高まっています。そして武力衝突の裏では、苛烈なサイバー攻撃が繰り返されるというのが現状だと思います。このことからも、今後は、サイバーセキュリティの検討において、日頃から有事を強く意識し、高い危機意識を持ち続けることが大切だと思います。

また、昨年はウクライナをはじめ世界各国がサイバー攻撃を受けました。これらの、攻撃の特徴・手法・成功した防御方法などの情報を、国際協力の枠組みを通じて入手し、国内の官民で連携して共有し、分析・対応能力の向上を図るとともに、来年度以降のサイバーセキュリティ計画に反映して頂けることを期待します。さらには、海外から得た情報ならびにその分析結果を用いて、本格的なサイバー演習・訓練を国内の官民、ならびに日本の関係国と共同で実施し、実際に起こりうる攻撃への対処能力の向上を図ることが重要だと思います。

2. 中小企業とサプライチェーンのセキュリティ強化

中小企業やサプライチェーンのセキュリティ対策は、サイバーセキュリティ2023(案)の「特に強力に取り組む施策」に取り上げて頂きました。これらは、日本の産業構造上、「最も重要」かつ「守るのが困難」な部分であり、業種によらずサイバー攻撃のターゲットとして狙われています。是非とも、これらのセキュリティ対策の抜本的強化を望みます。

日本の中小企業に関しては、非常に高度な技術力を持っている反面、資金面・人材面に課題があるというのが特徴であり、大企業へのサイバー攻撃が困難になるにつれ、攻撃のターゲットにされる機会が増してきました。中小企業は、大企業と違い専門家を育成し、網羅的なセキュリティ対策を行うことが困難なため、具体的な対策の提示と対策実施のための手厚い支援が必要です。今回、重要インフラのサイバーセキュリティに係る安全基準等策定指針(案)にランサムウェアへの具体的対策として「バックアップの復旧確認」「バックアップデータのネットワーク隔離」などが明示されていることは、中小企業にとっても非常にわかりやすい提示となると思います。

また、数年前からサプライチェーンを狙ったサイバー攻撃が増加していますが、組織の外部からの攻撃に対する防御力が格段に向上した一方、サプライチェーン経由の攻撃に関しては対策の漏れがあり、未だ脆弱である点が強く影響しています。サプライチェーンには、OSS を含むソフトウェアのサプライチェーン(SBOM など)、ハードウェア部品のサプライチェーン、企業間のサプライチェーンなどいろいろな繋がりがありますが、対策が現在進められている表面的・局所的な課題として捉

えるだけではなく、ヒト・モノ・カネ・情報などすべてを含めた組織間・地域間の広範囲の繋がり(チェーン)として改めてセキュリティ視点で見直し、検討する必要があると思います。

3. AI 等利用におけるデータのセキュリティ

昨年の秋以来、「生成 AI」が注目を集めています。特に、ChatGPT をはじめとする大規模言語モデルにおいては、我々の予想の上を行く会話能力を披露し、ビジネス界にも多大な影響を及ぼし始めています。同時に、新たに AI の普及が創り出すセキュリティリスクに関しても、専門家から指摘が出始めており、今後これらを検証し、対応していく必要があります。

これらの中で忘れられがちなものの 1 つが、制御システムなどにおける AI を使ったリアルタイムでのデータ処理です。今後、産業分野でも自動運転や電力制御など AI 技術の導入が急速に進むことが予想され、膨大なデータを基にしたリアルタイムな状況判断が人手を介さず行われるようになるのは確実です。今まで、人間が長年の経験に基づく総合的な分析によって判断していたことが、様々な機器やシステムから出力されるあらゆるデータによって導き出される「全体最適」で判断されるようになります。人間が行うのに比べ、より高速で広範囲な処理に基づく判断に移行しますが、同時に入力データに誤ったデータが混入していると、人間では起こしえないような誤った判断を行う可能性もあります。

AI を安全に利用するためには、入力データの信ぴょう性(完全性)の確認機能や AI などが行う判断の正常性判断機能など、しくみが必要不可欠になると思います。

以上